[H.A.S.C. No. 112–39]

IMPROVING MANAGEMENT AND ACQUISITION OF INFORMATION TECHNOLOGY SYSTEMS IN THE DEPARTMENT OF DEFENSE

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

HEARING HELD
APRIL 6, 2011

U.S. GOVERNMENT PRINTING OFFICE
65–810 WASHINGTON : 2011

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

MAC THORNBERRY, Texas, *Chairman*

JEFF MILLER, Florida
JOHN KLINE, Minnesota
BILL SHUSTER, Pennsylvania
K. MICHAEL CONAWAY, Texas
CHRIS GIBSON, New York
BOBBY SCHILLING, Illinois
ALLEN B. WEST, Florida
TRENT FRANKS, Arizona
DUNCAN HUNTER, California

JAMES R. LANGEVIN, Rhode Island
LORETTA SANCHEZ, California
ROBERT ANDREWS, New Jersey
SUSAN A. DAVIS, California
TIM RYAN, Ohio
C.A. DUTCH RUPPERSBERGER, Maryland
HANK JOHNSON, Georgia
KATHY CASTOR, Florida

KEVIN GATES, *Professional Staff Member*
MARK LEWIS, *Professional Staff Member*
JEFF CULLEN, *Staff Assistant*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2011

WEDNESDAY, APRIL 6, 2011

IMPROVING MANAGEMENT AND ACQUISITION OF INFORMATION TECHNOLOGY SYSTEMS IN THE DEPARTMENT OF DEFENSE

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

IMPROVING MANAGEMENT AND ACQUISITION OF INFORMATION TECHNOLOGY SYSTEMS IN THE DEPARTMENT OF DEFENSE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Wednesday, April 6, 2011.

The subcommittee met, pursuant to call, at 2:46 p.m., in room 2212, Rayburn House Office Building, Hon. Mac Thornberry (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. MAC THORNBERRY, A REPRESENTATIVE FROM TEXAS, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. THORNBERRY. The hearing will come to order. And we thank you all for your patience as we had some votes that have just concluded.

The subcommittee meets today to receive testimony on the impact of recent initiatives that affect the capability of the Department of Defense to acquire and manage information technology systems. The advent of the information revolution has not only changed how we as a Nation do business, but it has significantly impacted how we provide for the common defense.

Information technology includes everything from hardware and software, to data standards, to commonly agreed-upon architectural frameworks, and has completely permeated the national security enterprise, at least the information technology portion of the budget that has been submitted by the President. It is approximately $38½ billion, so a not inconsiderable sum of money. Obviously we are interested in how that money is spent, whether it is spent efficiently. Most importantly to me is whether it enables the warfighter to do what we ask them to do.

But as you all know, this subcommittee is also particularly interested in the security of our systems this year and cybersecurity for the Nation. So we are interested in what we are buying and how secure it is. So we appreciate our witnesses and the ability to discuss this topic today.

And I would yield to the ranking member, the gentleman from Rhode Island, for any comments he would like to make.

STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Thank you, Mr. Chairman.

I would also like to welcome our witnesses here today. It is good to have the Honorable Elizabeth McGrath and the Honorable Teresa Takai here, and I look forward to their testimony.

The issue of information technology is critically important to the Department of Defense, and I want to thank Chairman Thornberry for calling this hearing. IT [information technology] is a crucial factor in every aspect of the Department's activities. From the routine e-mail to the flight controls of the most sophisticated fighter jets in world, the Department depends on the smooth functioning of a myriad of IT systems. As the information age matures, we find that IT systems have expanded both in complexity and pervasiveness. As a result, today they represent one of the largest investments for the Department, and it presents a significant potential vulnerability if they should fail or be attacked.

The business complexities are only made worse by the evolving cyberthreats that have begun to challenge the integrity of our current systems. Therefore, it is important for the Department to be properly organized and pursue IT acquisition, implementation, modernization and performance evaluation. Oversight is required for the full spectrum of activities, but bureaucratic redundancy creates confusion and complexity.

Now, the DOD [Department of Defense] IT enterprise must be as streamlined and efficient as possible. I understand that as part of the Secretary of Defense's efficiency initiative, we will see some changes in how the Department manages IT and perhaps some cost savings along with it. Now, this is welcome news, provided it achieves the desired effect without reducing capability or injecting unnecessary risk into the process.

We must also be vigilant that as we move forward, the security of our systems is at the forefront of our efforts. Our acquisition systems furthermore are barely suitable to large-scale weapons projects requirements for IT systems that evolve rapidly, and the systems need more flexibility if it is to manage proper acquisitions of these systems.

As Mr. Thornberry mentioned previously, last year's 2010 National Defense Authorization directed the DOD to develop and implement a new acquisition process for IT, and I certainly look forward to hearing more about how that process is proceeding today.

With that, I yield back and look forward to our witnesses' testimony.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 31.]

Mr. THORNBERRY. I thank the gentleman.

It would be no surprise to you all that there are a number of meetings going on now, including a Republican conference on the funding situation with the government, so we may have Members coming in and out at strange times. But I appreciate your patience with that.

The witnesses today, as the gentleman mentioned, is the Honorable Teresa Takai, Acting Assistant Secretary of Defense for Networks and Information Integration and the Department of Defense Chief Information Officer; and the Honorable Elizabeth McGrath, Deputy Chief Management Officer of the Department of Defense.

Without objection, your full written statements will be made part of the record, and you are both certainly welcome to summarize them in any way that you see fit now. Thanks for being here.

STATEMENT OF HON. ELIZABETH A. MCGRATH, DEPUTY CHIEF MANAGEMENT OFFICER, U.S. DEPARTMENT OF DEFENSE

Ms. MCGRATH. Good afternoon, Mr. Chairman, Congressman Langevin. Thank you for the opportunity to discuss the Defense Department's efforts to improve its business operations, and specifically its acquisition and management of business information technology systems.

As the DOD Deputy Chief Management Officer, I am responsible for instituting a framework to define clear business goals, develop meaningful performance measures and align activities through established and repeatable processes. The purpose of DOD's overarching management agenda is the establishment of an effective, agile and innovative business environment that is fiscally responsible.

The Department has taken decisive action to improve its business processes, has identified areas where further work is required, and has several achievements to bring to your attention. My written statement addresses these in detail. I will briefly touch on some of these topics, as I am eager to discuss with you the areas that interest you most.

I would like to highlight our IT acquisition reform efforts, other business IT initiatives, and successful cross-agency management efforts in which my office plays a key role.

Fundamentally, the Department's business IT systems are essential enablers of a broader set of integrated business operations rather than an end to themselves. We have identified 15 essential what we call end-to-end processes, such as Hire-to-Retire and Procure-to-Pay. Our Business Enterprise Architecture and senior governance bodies, including the Investment Review Boards and the Defense Business Systems Management Committee, both given to us by Congress, are better aligned to manage within the end-to-end construct to identify data standards, performance measures and policies necessary to improve our business and make more informed enterprisewide decisions.

End-to-end focus and strong governance are joined by a new approach to acquiring information capabilities. There has been no shortage of studies and reports, including one by this committee last year, that concluded the Defense Department's current method for acquiring IT systems must change. Steps are being taken to address these issues.

Section 804 of the Fiscal Year 2010 National Defense Authorization Act required us to develop and implement a new IT acquisition process with its focus on the Department's IT Acquisition Task Force, which I chair. The guiding principles adopted by the task force incorporate recommendations from the Defense Science Board report, including deliver early and often, with delivery capability in 12 to 18 months; incremental and iterative development and testing; rationalized requirements; tailored and flexible processes; and

finally, a knowledgeable and experienced information technology workforce.

I welcome the chance to elaborate here on how the task force is addressing these areas. We expect to promulgate these in a policy later this year, such as establishing metrics to assess overall health of a program, combining certification and accreditation with traditional tests and evaluation activities, and assessing contracting strategies that enable a more modular delivery of capabilities. Our pilot-based approach to validate this new policy will allow us to modify as necessary based on lessons learned before the final issuance. We are currently testing these changes to ensure they are working.

The Under Secretary of Defense for Acquisition, Technology and Logistics signed out new acquisition policy for defense business systems called the Business Capability Lifecycle, or BCL, which provides a streamlined framework for development, testing, production, deployment and support of a defense IT business systems. The principal focus of Business Capability Lifecycle is program implementation.

In my written testimony, I have an example of an Air Force program that was originally on a path to deliver capability many years out. Using an innovative streamlined approach, we were able to move that deployment 2 years earlier.

I also welcome the chance to describe for you our cross-agency efforts in modernizing health information technology and security clearance processing. In particular, the Government Accountability Office's removal of the DOD Personal Security Clearance Program from its high-risk list is a significant first for the Department and owes its success to our commitment to this results-oriented, end-to-end approach.

In closing, we are committed to improving management and acquisition of IT systems, as well as our overall business operations. These issues received significant management attention and are a key part of our overarching strategy to build better business processes that will create lasting results for the men and women in uniform.

I look forward to continuing our work with this committee in the months and years ahead as we work toward greater efficiency and effectiveness and furthering the agility in the business space of the Department, certainly enabled by modern, interoperable IT capabilities. I look forward to your questions. Thank you.

[The prepared statement of Ms. McGrath can be found in the Appendix on page 32.]

Mr. THORNBERRY. Thank you.

Ms. Takai.

STATEMENT OF HON. TERESA M. TAKAI, ACTING ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION, AND CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF DEFENSE

Ms. TAKAI. Good afternoon. Good afternoon, Mr. Chairman and Congressman Langevin. Thank you very much for the opportunity to testify today on the importance of information technology to the transformation of the Department of Defense. My testimony today

will focus on how the DOD is leveraging information technology to securely deliver mission-critical information capabilities to the men and women of the Department of Defense and our mission partners.

The Department's fiscal year 2012 IT budget request, as you mentioned, of 38.4 billion, includes funding for everything from our desktop computers, tactical radios, identity management technology, commercial satellite communications, and the large information technology projects, some of which Ms. McGrath spoke of. These investments support mission-critical operations that must be delivered in an environment of ever-changing requirements and ever-increasing demand.

Where in the past the Department sought to balance the need to know with the need to share, today the warfighter expects to have and needs to have the latest information in order to complete the mission. That coupled with the increasing use of social media, smart phones and tablet computers has made information-sharing an expectation, and this requires new capability, particularly at the edge or in our tactical environments that have limited availability of persistent and broad-range network capabilities.

Our challenge today is ensuring our networks can securely support the information demands of our users, who require that information anywhere and any time across our enterprise. To meet this challenge, our networks must be designed and optimized to more effectively and efficiently support these mission operations while ensuring security.

DOD networks are under constant attack from cybersecurity threats launched from the Internet or from malicious software embedded in e-mail attachments, removable media, or even embedded in the hardware the Department procures. Every device connected to the network is susceptible to cyber vulnerabilities. While working to efficiently respond to the information demands of our users, we must be ever-vigilant in protecting our information environment.

Just over $2.8 billion of the Department's overall budget is devoted to information assurance or cybersecurity activities that defend our information systems and networks. The Department's fiscal year 2012 information assurance budget request ensures increased funding to address insider threat and cyber vulnerabilities, such as those identified in the WikiLeaks incident. Specifically, we have requested funding to support the deployment of a Public Key Infrastructure-based identity credential on a hardened smart card for use on our Secret classified network, a successful technology very similar to the Common Access Card we use on our unclassified network. We have also identified funds needed to deploy our Host-Based Security System to secure our classified systems; to provide an automated capability to continually monitor the configuration and security of our network; and improve identity management across the Department.

The DOD is planning for the investment and implementation of these IT and information-assurance capabilities within today's current resource-constrained environment. Recognizing this, in August, the Secretary directed a number of initiatives to achieve savings in acquisition, sustainment and manpower costs, while not de-

grading our ability to execute our mission. Among these is the consolidation of our IT infrastructure while simultaneously defending that infrastructure.

My office is responsible for leading the development of a strategy and plan for consolidating the Department's IT infrastructure in five broad areas: Our network services, our computing services, application and data services, our end-user services, and our IT contracts and purchasing. I plan to issue the DOD IT Enterprise Infrastructure Optimization Strategy this quarter. The plan represents the Department's strategy and initial roadmap to achieve the goals of improving our effectiveness while heightening our security posture. This plan commits us to changing policies, cultural norms and organizational processes to provide lasting results. The initial focus is on obtaining tangible results in fiscal years 2011 and 2012 while planning for aggressive consolidation through fiscal year 2015. It really positions us to embrace emerging technology and provide cutting-edge capability to our warfighters.

The transformation of our IT capabilities described above is a very ambitious undertaking, one that will reap tremendous benefits to the Department and our Nation when completed. It will require agility as well as new processes to both keep abreast of technological advances and defend the network.

My office is working closely with the Office of the Deputy Chief Management Officer on efforts to develop a flexible, agile acquisition process that also addresses the DOD's requirements and budgeting processes.

As you know, we have also been addressing the development, education and continuous training of our workforce. The Information Technology Exchange Program pilot reauthorized by the fiscal year 2010 National Defense Authorization Act for DOD is one mechanism that we are pursuing. Under this collaborative effort, we have a pilot which will involve 10 individuals exchanging both industry and Department expertise to enhance our employees' IT competencies and technical skills, and infuse both DOD and the industry with new ideas in this fast-evolving discipline. My office is responsible for implementing ITEP [the Information Technology Exchange Program], and we have created a guide to assist participating DOD components with the implementation.

Maintaining an information advantage for our users is critical to our national interest. The efforts outlined in this brief will ensure that the Department's information capabilities provide better mission effectiveness and security and are delivered in a manner that makes the most efficient use of our resources.

I want to thank you for your interest in our efforts, and I am happy to answer any questions that you have.

[The prepared statement of Ms. Takai can be found in the Appendix on page 44.]

Mr. THORNBERRY. Thank you.

Let me start out with, I guess, some rather broad kind of questions. Ms. McGrath, about 10 years ago, the Defense Science Board did a study that found 16 percent of all IT projects complete on time and on budget; 31 percent were cancelled before completion; 53 percent were late and over budget. Of those that were completed, the final product contained only 61 percent of the originally

specified features 10 years ago. How much better is it now, do you think?

Ms. MCGRATH. From a percentage perspective, I don't think I would be able to articulate percentage-wise how much better I think it is. I do think that the Department is taking a more holistic look at how IT fits into our broader capability needs. I would say 10 years ago, we would have a handful of people who are interested and focus on how IT worked and enabled in the entire environment, and today we are taking a much more enterprise perspective.

I can talk about the many studies and reports that have been done in terms of how the acquisition process needs to be better to enable a more rapid capability and delivery of the information technology. Maintaining a standard, stable baseline of requirements, I think, can be found in every single one of the studies and reports that have been completed. So a lot of the focus of the Department not only on the IT side, but the weapon systems side has been to identify and stabilize those requirements such that we can meet them in a more—I am going to say to chunk the capabilities such that they are delivered in a spiral fashion and not try and solve the entire issue at the get-go.

So, you know, percentage-wise, specifically I am not sure how to counter those numbers that you articulated, but I can say certainly within the last 5 years that there is a lot more management attention and focus on the requirement stabilization, the spiral implementation so that I do feel that we are moving in the right direction.

Mr. THORNBERRY. And I want to talk more in a minute about some of the acquisition points that you make.

Somewhat on behalf of one of my colleagues, let me ask you this: From time to time, we have asked about the ability of the Department of Defense to withstand an audit, and a lot of the answers that have come back to me over the years is, well, we just don't have the computer systems that can talk to one another, you know. So basically the business systems were not compatible in order to put all the pieces together. And I realize it is not your responsibility to audit the Department, but just from the business systems technology part of this, where are we now?

Ms. MCGRATH. And I would agree, the systems were designed very locally and not with a broader auditability target in mind, nor with a common architecture framework in mind. So they were local solutions to handle local problems to do the sort of the math, if you will, accurately.

Today the environment is very different. With the Business Enterprise Architecture standard—financial information of standards, a standards-based approach to implementing these Enterprise Resource Planning solutions, we have many ERPs within the Department that will contribute to the Department's ability to achieve financial auditability, and they are a very key factor in our success in that pursuit. And we do recognize that it is a business goal, a broad business goal, not just an IT problem, nor is it just a comptroller problem, but it is a shared responsibility across the functional space, meaning, you know, logistics, personnel. They all have a part because their transactions are where it all starts and then end up in the financial system at the end of the day.

So we are taking, again, a very deliberate, cross-functional enterprise approach to not only the IT aspect of it, but the business process, because it requires change in all of those areas.

Mr. THORNBERRY. Well, I know there are a number of people on the committee as a whole that wants to hasten the day when that is possible. So I appreciate that.

Ms. Takai, I guess the first question that leaps out at me for you is do you have the authority to do your job? And you said, I think, in your testimony, this includes everything from radios, to laptops, to the desktop computers. All of those spending decisions are made by the services or other entities. You are there kind of to help coordinate or strategize or guide, but they don't have to listen to you. Do you have the power to do your job?

Ms. TAKAI. There are a couple of answers to that question. So let me phrase it in a couple of different ways.

Certainly while the budget dollars for the information technologies expenditures are in the services, there are any number of the processes in the building that actually review that spend where my office has a major role. Certainly in the requirements process that Ms. McGrath talked about not only from a business systems standpoint, from also the standpoint of to the point of command-and-control systems for things like tactical radios, my office is involved in the review of those programs and certainly have the opportunity at that time, based on a technical review and based on just an overall project review, to weigh in on those projects. So there are those processes. There is also, obviously, our investment process through the CAPE [Cost Assessment and Program Evaluation] organization, where we look early on at our investment decisions.

So while, in fact, we don't control the overall budget, there are requirements and investment processes. And then ultimately in the acquisition process, we are also a member of the groups that actually review the projects going through. So we do have opportunities certainly to weigh in.

The other piece of it is that in our responsibilities, they are very definitely two-set policy, and in setting that policy, we are doing that, as I mentioned in our IT consolidation plan, in ways that actually direct the expenditure of the dollars, even though it resides within the services.

Mr. THORNBERRY. And through these various committees and all this stuff that you sit on—let me ask this: How often is your organization's judgment overridden, would you guess?

Ms. TAKAI. I wouldn't have a good view of that. I am fairly recent, as you know. I joined the organization in November, and so I don't, you know, actually have very real specifics or percentages or anything at this time to be able to give you.

Mr. THORNBERRY. On the integration strategy that is coming out this quarter, is that going to be classified or unclassified?

Ms. TAKAI. No. It will be available. And certainly as we complete it, it would be something we would very much like to share with you.

Mr. THORNBERRY. But there will not be a classified version of it.

Ms. TAKAI. No.

Mr. THORNBERRY. Okay. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Again, I want to thank you both for your testimony here today.

Secretary Takai, I want to thank you for what you have had to say today. I would like to in particular discuss a major concern that I have about the Department's information technology consolidation. As you are aware, the Administration's Chief Information Officer, Vivek Kundra, if I pronounced that correctly, instituted a Federal cloud computing strategy in February, which mandated that all agencies modify their IT portfolios to fully take advantage of the benefits of cloud computing in order to maximize capacity, improve flexibility and minimize cost.

While the benefits from cloud computing can certainly be great, I believe that the security of cloud architecture isn't fully understood, and remain very concerned that organizations may ignore security concerns in an effort to rapidly glean the vast cost savings available from migrating to the cloud.

So further, the discussions of specific items such as how cloud computing will affect law enforcement, intelligence organizations hasn't also been fully analyzed as well in depth. Companies that suggest cloud server farms can be adequately secured overseas really aren't discussing the complex requirements for background checks and foreign servicing personnel or our ability to work with foreign governments to access data harmful to the U.S. when it resides on the same server amongst benign data from a foreign country.

So, Madam Secretary, with these concerns in mind, what assurances can you give this committee that all aspects of security will be considered, discussed and planned for in advance of DOD's IT migration to the cloud?

And second, as DOD begins its migration, is there a discussion of where data farms will reside? And if so, does that discussion include the Department of Justice and members of the Intelligence Community?

Ms. TAKAI. Well, thank you very much for that question, because I think there is a significant amount of confusion as we talk about cloud computing. It has a tendency to mean different things to different people. So I think it is very important.

You know, while we certainly agree with Vivek Kundra's assessment that there are opportunities, we also believe that we have to look at the way we move to the cloud in several different ways. And security is actually our paramount concern in terms of the way we look at cloud computing. So let me put that in our overall context.

Our initial look at moving to cloud computing would be to look at what we call a private cloud. So it would effectively be taking the benefits of cloud computing, but rather than looking at how we would buy that service outside, to look at the way we would standardize our infrastructure, the way that we can utilize the organization like DISA [the Defense Information Systems Agency], which has several large computing centers today, and actually be able to bring in implementations from the services, for example, be able to get the cost-effectiveness, but at the same time be able to assure the securities.

So, for instance, right now Army is looking at a number of applications that they will be moving into a cloud where we will have full control of the security, including the points that you raised as it relates to the security required for employees, where we actually locate those centers and also the information that we have in those centers. So our initial foray, again, is to ensure that security is our number one concern in terms of being able to move forward.

I think, as you mentioned in your opening remarks, while, in fact, efficiency is extremely important to us, we have to be sure that both from a security and protecting the warfighter that we are fully capable.

Now, there will be instances—and we are looking at those now—where we will be able to use commercial cloud providers. But when we do that—and, in fact, this is a conversation that I think Vivek Kundra is looking at as well—we will have to be sure that those providers meet our security standards before we will utilize those services.

And then lastly, we are looking now because we believe that there may be a few instances where we can go to a public cloud, but they would be for those things that don't require the kind of security on our networks and from an information perspective. And so those are the ones that we are taking a look at as well.

So I do think while we are looking at this, it is important to put it in the context of the different types of cloud-computing environments and the fact that we are actually driven in terms of our making the decision by our security concerns and our standardization issues as much as certainly from the standpoint of efficiencies.

Mr. LANGEVIN. So in that process, as you are moving to the cloud architecture, will that include discussions with the Department of Justice and also members of the Intelligence Community?

Ms. TAKAI. Absolutely. One of the concerns that we have right now, in fact, is being able to take a look at our information-sharing capability across the networks that the Intelligence Community is responsible for and the SIPRNet [Secure Internet Protocol Router Network] and NIPRNet [the Non-secure Internet Protocol Router Network] that we are responsible for. So as a part of our ongoing planning, it is very important that we are well coordinated with the Intelligence Community. And as they are looking at where they are moving forward, I think in conversations I have had with them, certainly security is also their number one concern.

In answer to your second part of the question, which is Department of Justice, obviously with some of the challenges we have had from an insider threat perspective, it is very important that they be involved in any decisions we make about the location and the configuration of where we put our information.

Mr. LANGEVIN. If I can continue. Another area of concern is DOD's ability to continue its information-sharing efforts. As we are all aware, the 9/11 Commission highlighted some serious interagency deficiencies as to the timely sharing of sensitive information. Since that time, much of the Federal Government has made significant improvement, yet I am concerned that the insider threat-type setback, such as the WikiLeaks affair, is going to hamper further efforts to improve the sharing of threat and intelligence

information across the spectrums of threats both physical and cyber amongst agencies.

So, Secretary Takai, does the DOD have the capability to track insider threats to our information systems, particularly those processing classified information? And what effect has the WikiLeaks case had on our information-sharing efforts both internally as well as interagency?

Ms. TAKAI. Well, let me answer that, first of all, by saying we are continuing to be focused on information-sharing. And it has been a major concern for us to ensure that we can do that information-sharing in a secure way, because, as I mentioned, we feel that certainly for the warfighter, the need to have access to that information has never been more important than it is today. So what we take as our responsibility is to be sure that we can do that information-sharing in a secure manner.

And that is really why I mentioned several areas of technology that we are implementing so that we can continue to do that sharing, and yet do it in a secure way. One of the tools that we are deploying at this point in time is our Host-Based Security System. And that is really, again, in response to your question about knowing who is on the network and knowing who has access to information.

We have two additional tools that are going to be very important in actually helping us with that. We are currently testing a tool and plan to roll out a tool which will actually detect what we call anomalous behavior.

So to your question of do we know who is on the network? Yes. And then what we need are tools that begin to detect where there is access to information that looks different than what we would expect to see and then will trigger our ability to get in and take a look at that.

Then we are deploying much stronger identity management capabilities so that we will be able to tag information to particular users and then be able to continue to protect.

Now, while these technology enhancements are extremely important, we also are improving our processes and our procedures for access to that information. So I think, as you know, we have put policies out about the use of removable media, but to ensure that the warfighter has the capability to see that information, we have also instituted processes, for instance, which is a two-person rule around access to information so that we are sure that there is always a check and balance when there is the need to know.

So again, to summarize, the challenge for us is to put the technology in place, but also, because there is never a 100-percent solution, to be sure that we also have the policies and the processes in place to be able to manage our information.

Mr. LANGEVIN. I have further questions, but thank you for that, and I will wait until maybe a second round.

I yield back.

Mr. THORNBERRY. Thank you.

Mr. West.

Mr. WEST. Thank you, Mr. Chairman, and, Mr. Ranking Member. And, ladies, a pleasure to be here, and, Secretary, and Honorable McGrath.

I spent a few days in the military myself, and I can tell you when I first came in, you know, everything in the artillery was charts and darts, and now everything is computerized. And, of course, I was in Desert Shield, Desert Storm where you stood in line for about 3 hours to get, you know, a 2-minute phone call.

I spent 2½ years in Afghanistan. I can tell you from the experiences then to now, information technology and the network systems that we have deployed in these combat theaters of operation are just incredible. But one of the things that I know that we have to also be able to do is to protect those systems in a combat zone, which is something we experienced for about 48 hours in Afghanistan. I think you know what I am talking about back, I believe, in 2006, and we were able to trace that back to a very interesting country.

So one of the things I look at as we go probably from, you know, so much of nation-building, so much of occupation-style warfare, and we get back to maybe power projection, forceable entry, more austere environments, what lessons have we learned in the operations in Iraq, the operations in Afghanistan that will make us better prepared, make us, you know, more secure with the implementation of our network systems as we move forward, you know, Libya, Tunisia, who knows where is next?

Ms. TAKAI. Well, just some examples, I think, to add to your comments, which I think really do reflect the changes that we are seeing actually in theater. First of all, we are seeing very definitely that our need for network security going forward needs to include our coalition partners. And so what we saw in Afghanistan was the need to actually put a network in place that allowed for each of the coalition partners to have their own secure network, but at the same token have a network which was protected at the point that each of our coalition partners connected to it so that if, in fact, we had an issue at any of those points in time, we could then block that and not have that impact the entire network.

One of the things that we see going forward is that we have to be cognizant of several things: Number one, what I just mentioned, that while we might not necessarily deploy the technology in the next conflict in the same way we did in Afghanistan, we certainly would deploy the concepts that we are using there, again because of the coalition.

The second piece of it is that what we have seen is the need to share information—and this really gets back to some of the other questions—across our unclassified and classified networks. While we have seen that in the past, I think we haven't seen it to the extent that we are seeing it today. And so our future networks will need to plan for that level of information-sharing.

And then lastly, these tools that we are putting in place now are really aimed at being able to better secure these networks when we go in.

And then finally, what we are really recognizing is that we have to standardize our networks because it is not just the networks, but it is what folks want to connect to the networks. And they are bringing any number of devices. They are familiar with devices, commercial devices that just weren't even things that were conceived of being used in theater, and they are bringing them with

them. They are used to them. They don't stand in line to make a phone call. They have a device in their hand.

Mr. WEST. You are absolutely right.

Ms. TAKAI. And we have to recognize that that is the situation, but the challenge for us is ensuring that when they do have access to the network, they have access to the network in a secure way. So it isn't then everyone can bring anything they want, but they have to have that capability, and our networks have to be secure enough to sustain that.

Mr. WEST. And, Ms. McGrath, a question. In the aftermath of what we saw with the WikiLeaks, have we gone back and really looked at our, you know, security clearance processes? You know, have we gone back to some type of retraining, recertification process?

Ms. MCGRATH. With regards to the Federal investigative standards, those have been looked at by both the security executive agent, which is the Director for National Intelligence, and also the suitability executive agent, which is the Director for Office of Personnel Management, to ensure that when we are pursuing either a hiring action or a clearance determination, that we have done the appropriate level checks for the level of access or job that that individual will have.

So we have, from a Federal perspective—not only just DOD, but this is a much broader Federal—paid attention to the information that we gather to ensure that we are collecting the right information to make those determinations. And we also applied some of the sort of innovation and technology to that process because historically it has taken much, much too long to obtain a security clearance. So we did, through process analysis and innovation and technology, apply those appropriately to the process to enable speed without degradation of quality.

Mr. WEST. Thank you very much.

And I yield back, Mr. Chairman.

Mr. THORNBERRY. Thank you.

Mrs. Davis.

Mrs. DAVIS. Thank you, Mr. Chairman.

And, Ms. McGrath, thank you very much, both of you, for being here, Ms. Takai.

One of the discussions that we have been having in the personnel committee over quite a number of years is bringing together electronic records, of course, of the DOD and the VA [Department of Veterans Affairs]. And I see that in your written testimony you alluded to that, and I am sorry I wasn't here at that time. It is my understanding that there are three options that they were looking at, and how is that progressing, and what are those options, I guess? And what does the timeline look like that might bring us to a decision?

Ms. MCGRATH. The "they" you are referring to in my assumption is both Secretaries Gates and Shinseki recently met. Actually it was on March 17th. We gave them a presentation. We did look at options in determining our collective way forward for electronic health records. One was looking at upgrading our existing capabilities. DOD uses AHLTA [the Armed Forces Health Longitudinal Technology Application], and the VA has VisTA [the Veteran's

Health Information Systems and Technology Architecture] as their major IT system. The other was taking a joint approach to a—I will use the term "single solution," but I really mean single approach to capability delivery. And the other one was pursuing our own separate IT capability initiatives with a bridging mechanism to share data, which is mostly how we interface and exchange information with VA today. So those were the options that were discussed with the Secretaries.

The decision was that we agreed to use a common architecture, common data services and data centers, and it would be a standards-based approach to exchanging data as opposed to the interfaces that we do today. So it would be a data-driven approach to information exchange.

We have agreed to joint development/acquisition, and it is probably more acquisition than development because there is a lot of commercial-off-the-shelf capabilities; a number of the functional areas, like pharmacy and labs and those kinds of things.

For an integrated electronic health record, we will look at using commercially available solutions first, adopt an application if one of us has a best-of-breed that we are currently using. And then finally, our last option would be we would develop it.

In saying that, the difference really is that we are taking a lighter architectural approach as opposed to a heavy systems-based approach. Today our data and system are very much integrated, and so it limits our ability to be agile and exchange at the data level. The major difference in the approach that we are taking is exchange at the data level. That will require us to develop this common architecture that is a significant difference in how we do things today.

Governance will be key going forward, having the effective governance in place to ensure that we are staying aligned to the agreements that had been made by the Secretaries, and also with regard to the capability we have currently deployed in the North Chicago Medical Center. We have agreed to pursue any capability that is not yet delivered there, pharmacy and consults being the major two, to pursue those jointly.

Saying all that, those are the agreements that we reached. We have a comeback to the Secretary, both Secretaries, early in May where we are to deliver more details with regard to the implementation timeline.

Mrs. DAVIS. Are there any steps that either the DOD or the VA are taking now where their efforts essentially would not be very productive if they move ahead in the separate ways that they have been moving all these years? I guess are there certain investments, certain expenditures that are moving forward in the different architectures that would not necessarily mesh with what may eventually be the——

Ms. MCGRATH. The message is to ensure that the investments that we are making in today's environment are needed today. And if there are things that we can defer such that we ensure alignment with this integrated electronic health record, that is what we would like to do. North Chicago is a really good example. Each of the departments was pursuing a separate pharmacy solution that

would interact through interfaces. We have stopped those separate development efforts, if you will, to ensure that we pursue——

Mrs. DAVIS. I guess can I ask you, given the cultures and given the difficulty with getting to this place, how successful are we going to be?

Ms. MCGRATH. I mentioned the governance. Governance is key, and the agreements by the Secretaries and then the persistent engagement by the Secretaries I think will be key to enabling success here. Both Secretaries have agreed to continue to monitor the progress that the two Departments are pursuing, in addition to the Deputy Secretaries of both organizations and our Joint Chiefs of Staff.

Mrs. DAVIS. If you were overseeing this, and as a committee, what would you want to see in 3 months and in 6 months from now? Where should we be?

Ms. MCGRATH. Those things that we have currently agreed to with regard to the data standards and data center consolidation, certainly we should be able to provide plans and enter milestones on where are we to achieving those goals. I certainly would ask for those. Those are things that we will be delivering to the Secretaries. And we will need those in place to then be held accountable to managing towards—you know, to achieving the overarching goal. And I think that as we define how we are going to pursue different capabilities, certainly, you know, cost and schedule for all of those are absolutely what I would ask for.

Mrs. DAVIS. All right. Thank you. I appreciate that.

As you can sort of sense my impatience here because—aside from the fact it is very costly, I think, just to the government, to all of us, it is also costly to the warfighter. And we know that we have been working at this for a long time. So I am really hopeful that we can have a deliverable soon.

Ms. MCGRATH. I would just like to add, we do between the two Departments share so much data today with regard to the medical. I mean, it really is incredible when you look at how much data the two Departments share today. What we are talking about is enabling the sharing of that information, taking a different approach from a data perspective so that we can eliminate redundancies, you know, increase efficiencies so it is a better experience for our military members.

Mrs. DAVIS. Thank you.

Mr. THORNBERRY. Is that a 3-year project or a 10-year project?

Ms. MCGRATH. I don't think it is a 3-year project to be completed, but I do think that there are, again, phases of implementation we will be able to achieve in terms of the data standards. There are already international health data standards out there. DOD has already enabled standardization within our own enterprise. It is aligning with VA. I don't see that as—certainly not a 10-year. So I actually think that we will be able to achieve some of that interoperability much sooner than the 10-year mark. So I do think that there are some opportunities in the nearish term, the near being relative, to achieve greater interoperability than we have today.

Mr. THORNBERRY. Thank you.

As you all know, one of the provisions of last year's bill was to provide the Department some rapid acquisition authority. I think

maybe you both make reference to it in your written statements. But can you update us on where that is? Is it being used? Have we gotten far enough to know whether it is the kind of authority you need?

Ms. MCGRATH. I can start, and certainly Ms. Takai can add on to my initial comments.

We have established—as the lead for the IT Acquisition Task Force—and the Department is certainly working very closely with Ms. Takai's office and our acquisition, technology and logistics organization, and, frankly, every organization, it seems like, within the Department from a test and evaluation to the comptroller, because we are all somehow involved in enabling delivery of capabilities with regard to our acquisition process.

We have established many work groups; focus on very specific areas like measures, metrics, what are leading indicators that we should be looking for when things are in a particular program to ensure that we achieve better outcomes; combining the certification and accreditation for testing with the regular test process. Typically we treat them separately, and they are not concurrent; they are sequential. So we are looking to take that timeline significantly down.

Taking a much more portfolio-management approach to overseeing these IT investments so that we are not just looking at one system at a time. We are looking at how does this one particular system fit within the broad portfolio within which it will be deployed, but also what other systems do we have that also utilize that same capability, how many financial systems do we really need. So you can look at it from a functional perspective and also within an operating environment.

Requirements I think I mentioned. Every study says that we don't baseline the requirements, we don't hold them stable. So we are ensuring that when we pursue a new IT solution, that the requirements are small enough that you can deliver them more rapidly in a 12- to 18-month timeframe. Typically we put all the requirements in one big bucket, and it is 5 years before we hit our initial operational capability. So in order to make those timeframes smaller, we need to parse the requirements such that we are delivering incremental capabilities.

Contracting is also an area that we are extremely focused on. I don't think there is anything within a FAR, Federal Acquisition Regulation, rewrite that we need. I think we need to be more creative about how do we utilize the contracting aspects, authorities that we currently have. But we need to contract differently than we currently do today. On the one hand, some programs will be a firm fixed price, but if you don't have your requirements nailed and definitized enough, fixed price is not the right way to go. But then time and materials does not seem like the most accountable way to also pursue an IT solution. So it is coming up with the balance, when should you use those types of contracting, and understanding that not one size fits all.

And then the other very key is the IT acquisition workforce. The Defense Acquisition University has a program management course down there. It is terrific, and I happen to be a graduate. But they don't teach IT the way we procure IT today. These enterprise re-

source planning program systems capabilities didn't exist previously. And so it is really putting a very fine point on our acquisition workforce to say, hey, IT today is very different from source lines of code and function point counts that we used to do. We are actually buying a lot more commercial-off-the-shelf capability and ensuring that we have got the right credentials for those folks.

We are taking very much a piloting approach. In my written testimony I highlighted an Air Force financial system called DEAMS, the Defense Enterprise Accounting Management System. We did utilize some of these different approaches to move their implementation significantly forward. Both Army and Air Force have their integrated personnel and pay systems. We are looking at establishing their acquisition strategy aligned with the more streamlined capabilities. The same with the Joint Space Operation Center mission system and the Navy's intelligence, surveillance and reconnaissance capability.

So we expect through the use of pilots we will learn more to ensure before we institute our final policy we have actually tried it out a little bit to see where we need to course correct, and so we get some fact-based feedback to ensure that we have policies that are in line with where we want to go.

Mr. THORNBERRY. Ms. Takai, it seems to me that, having heard all of that, it just seems very difficult for the Department to keep up with the change in technology, the way technology changes and with all that has to go on before a purchasing decision is made. So does that mean we are always going to be behind?

Ms. TAKAI. Well, it doesn't always mean we are going to be behind. There is a qualified answer to that, if I could add to what Ms. McGrath was talking about. And let me add to that, in addition to the many process changes that we have been working with her team on, we also believe that the efforts around streamlining and standardizing the technology we use are a critical part of being able to get innovative technologies in more quickly.

Right now what we do is we reinvent, in many cases, the same technology platforms over and over again because we bring them in in separate instances for separate projects. And so just as an example, you know, as we have been working together from the standpoint of business systems, if we can get standardized platforms, then it really does give Ms. McGrath an opportunity to build on those standard platforms and not have to worry about the technology coming in the door, but to be able to spend the money and the resources on understanding what business processes have to ride on it.

The second piece of that, though, is that if we can standardize and improve the security of our backbone, we can then look at more innovative technologies and not have to invent them all the way from the data center, the server, the network out, but rather look at how those innovative technologies can hook into our standard infrastructure. It gives us more flexibility in looking at those kinds of capabilities.

Having said that, as we build that out, we will need to, as Ms. McGrath mentions, look at shorter timeframes for bringing these technologies in. We will need to look at our testing and accreditation processes, because that is one of the inhibitors that we are

aware of today in terms of retesting platforms for every upgrade as opposed to recognizing that there are standard platforms and there is not the need to test.

So some of those things are the things that we are looking at from an information assurance perspective in terms of the policies that we put out as well as the accreditation and the testing that we do at DISA to, again, allow for bringing new technologies in, but at the same token making sure that when we do, we aren't increasing our risk from a security perspective.

Mr. THORNBERRY. And I guess related to that, what are your concerns about supply chain? You know, in general in cybersecurity we hear more and more concern about so many pieces of hardware and software that are not made here, and certainly many components are not made here. But as you and Mr. West were talking, you know, we have got soldiers out in the field that are taking whatever they have got out of their pocket to do their job or to communicate back home. That has got to create all sorts of challenges for you in looking at the overall enterprise.

Ms. TAKAI. We totally agree with you, and there are really two answers to the question you are asking about supply chain. One of them is just an awareness of the issue that you have mentioned. And we have two programs that we are working with NSA [the National Security Agency] and also with our policy office. One of them is to actually look at the ground rules around the way that we bring technology in and the, if you will, background information that we gather on the companies that we purchase from. So that is a key part of what we do. And, of course, in that, we are aided by information that we get through our intelligence sources as well about those particular companies.

The second thing from a supply-chain perspective is to work with our defense industrial base. And we have any number of programs that Deputy Secretary Lynn has been really spearheading around how to work and share information effectively with our defense industrial base, because, again, the supply chain problem isn't really just an issue of DOD. It really involves our key partners.

But the other piece of that is to recognize that as we move forward, and as there is obviously a globalization and a dispersion of where the information—or rather the components from a hardware and software standpoint come from, it is really to look at cybersecurity in that light, which is why we are focused not only on protecting at the perimeter, which has been a focus, I think, for everyone in terms of trying to prevent intrusions, to prevent invasions in your network. And now what we are recognizing is that while that is still a deterrent, it is not a complete answer from a security perspective. And so we have to look more at the way that we are classifying our information, the way we are linking that to the identities of the individuals that can access it. So, again, we have a second level of defense actually at the information level, and that we are acknowledging that we will have some of these kinds of intrusions inside our network, and we are prepared to handle them.

Mr. THORNBERRY. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

One last here that I wanted to talk about is the depth of DOD's bench in IT career fields. Secretary Gates' IT initiative—I realized

individuals assume that the new IT positions after efficiency implementation would require greater technical expertise and experience to efficiently maintain the Department's IT needs across all of the military branches. In the fiscal year 2009 NDAA, the committee directed DOD to look at the feasibility of identifying and retraining, for example, wounded servicemembers in information technology and other fields.

So my question is considering the challenges recruiting a competent IT workforce, have you leveraged any of those programs to help build your workforce there, and is there more that this committee can do to retain the skills and expertise of these wounded warriors to help meet our needs for a trained IT workforce?

Ms. TAKAI. Well, we have been moving forward in terms of looking at those individuals that are returning from theater, and particularly the wounded warriors programs, around the capability and making sure we have technology skills. But going forward we will continue to be vigilant and need to be vigilant on this. And while it involves, I think, as you mentioned, being sure that we are retaining and training our workforce, it also is a focus for all of us in terms of making sure that we have enough professionals coming up that are educated in cybersecurity and certainly educated in the sciences and the maths.

So some of the things that we are doing in that regard is to participate in and encourage many of the cybersecurity programs that are focused on our high school students as well as our university students, to get them interested at a very early age in a career in the science and maths, and particularly moving into cybersecurity. That is something that my office is very heavily engaged in, something that the policy office is very much engaged in. So it is going to be a combination of retaining the workforce we have, being able to grow it, but also making sure that we have an influx of individuals that have those skills.

Mr. LANGEVIN. Let us not at all forget about our wounded warriors and see how they might be incorporated into these job opportunities. I think that would be important.

I am also glad to hear that you have a focus on bringing up the next generation, whether it is focusing on high school or college. I actually starting working with the SANS Institute. We created the cybersecurity challenge at the high school level. My home State was one of three of the pilot States that originally tested the program through high schools in our State, and now we have kicked it off statewide. And it is amazing how talented these young people are. And the cyber challenge sets up the different hurdles that they have to kind of work through and test their skills, and hopefully get some on the career path, thinking about a career path in cybersecurity.

Ms. TAKAI. Yes, sir. And I just came, I think, as you may know, from the position of the CIO in California, and we were very much able to take advantage of that cybersecurity challenge program. And, in fact, I think we were the first to institute the high school version of that program, in order to be able to bring young people in and get them interested.

Mr. LANGEVIN. Very good. If I could, just going back to Congressman Thornberry's line of questioning. You talked about the supply

chain. And I actually had Secretary Lynn in my office yesterday, and we were actually talking about the supply chain industry. We were also talking about working with the defense industrial base and how do we best work with them on a voluntary basis to better secure their own networks.

And I was curious, when you say you look at companies you are doing business with, and you look at from the supply chain perspective, how far back do you drill down with each of those companies? The problem is not just the company that you are doing business with, but it is who they are doing business with and who they are doing business with. Since the supply chain can cover a range of problems, you know, it is not just the initial companies, but where are they getting the products from as well. So I guess how deep does that go?

Ms. TAKAI. The initial pilot that we did did not really—and I am sure that Secretary Lynn mentioned to you—we were able to go down deep in some companies. But when we really looked at the level of resource that was needed to actually be able to do all of that research, we recognized that we will be able to do a certain amount through research, but in many ways it is not going to be the full answer to looking at how we do supply chain.

And that is really why we are taking now a step back from that. We know we have to do a certain level of that, but it is also going to be we are not going to be able to do all of the research; we are going to have to engage with our partners.

And then, lastly, we are going to have to have other ways of looking at how to defend. Because I think your point is very well taken. You really can't have enough resource to be able to go down to every last component, and so you have to look at the major components, but yet that doesn't give you the complete picture. So that is why we are looking at not only being able to do that kind of research, but also recognizing that when we have threats inside our network, we are going to have to be able to mitigate them.

Mr. LANGEVIN. Fair enough.

And the last area of questions I want to get into, something in addition to and very much tangential to cybersecurity is the security of our military bases and critical infrastructure that supports our military bases. As you know, much of our critical infrastructure is owned and operated by the private sector. I am becoming increasingly concerned about Supervisory Control and Data Acquisition attacks in particular on critical infrastructure, particularly the electric grid. Our military bases around the country so much rely on these outside power grids for their own power, and I have been involved with reviewing how secure those bases are.

I have the chiefs of the services before us, and I have asked what their level of knowledge is on this, and it is troubling to them certainly as well. Our bases are not independent of the power grid. So I know this is a bit outside your area in particular, but it does relate to IT and cyber.

So in your work, do you have anything to add, any awareness that you have, on what we are doing to better secure our military bases in the event that something happens to critical infrastructure off the base and how they would be affected?

Ms. TAKAI. Well, let me add to the discussions. I know you have talked with Deputy Secretary Lynn about this. One of the things that he has been spearheading is to work very closely with the Department of Homeland Security for exactly that reason, because while clearly it is the Department of Homeland Security's responsibility to look at critical infrastructure as it relates to certainly the U.S., at the same token it does affect our military operations in those cases. And so what we are doing is to really work collaboratively with them around taking a look at those threats, being able to share information.

I think, as you know, there has been a close working relationship between Secretary Gates and Secretary Napolitano around the sharing of that information. And one of the things that we will be moving forward on as part of what Secretary Lynn calls our enduring security framework is now to move more into review of critical infrastructure protection, including not only our power grid, but also taking a look at some emerging areas, particularly, for instance, with nuclear power.

Mr. LANGEVIN. Very good.

Thank you, Mr. Chairman. I yield back.

Mr. THORNBERRY. Thank you.

Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman, for holding this hearing.

Secretary Takai, three intelligence contractors named HBGary Federal, Palantir Technologies and Berico Technologies have a proposal under the name Project or Team Themis. Are you familiar with this proposal that has been purportedly made by those three firms, all of which are defense contractors? Are you aware of that proposal that was leaked from the HBGary Federal e-mails which would offer the counterterrorism and intelligence techniques to prospective private parties, i.e., Bank of America, U.S. Chamber of Commerce, for use against critics of those firms? Are you familiar with that situation?

Ms. TAKAI. No, sir, I am not familiar with that specific proposal. So, you know, we are happy to take that for the record and gather that information and be able to get back to you on it.

Mr. JOHNSON. Well, now it has been about 2 weeks I requested that information. Do you know what has happened to that request and whether or not it is being complied with, or there is an intent to comply with it?

Ms. TAKAI. No, sir. I don't have that information. I wouldn't want to give you something that was incorrect. I will make sure that my office takes a look at it, and that we get right back to you on it.

Mr. JOHNSON. Now, it is my understanding that the firm HBGary Federal had developed malicious software that allows users to monitor the networks and computers used by third parties. Is that the kind of capability that they have provided to the Department of Defense?

Ms. TAKAI. Again, sir, I am not familiar with that company. So, again, my staff will definitely get that information and make sure that we get right back to you.

Mr. JOHNSON. If there is a misuse of properties of the Federal Government paid for by citizens of the United States through their

tax dollars, i.e., tools to disrupt foreign intelligence, foreign terrorism, and if that technology is used on Americans, would that be a breach of the contract between DOD and any particular contractor? Are there provisions in the contracts that prohibit such use?

Ms. TAKAI. Again, I would need to go back and take a look at that specific instance and get that information back to you.

Mr. JOHNSON. You do agree that that is a problem, that we should not use taxpayer-funded techniques on taxpayers who may disagree with a private domestic business entity?

Ms. TAKAI. Well, we at DOD are concerned with any breach to our networks or any risk to the security of our information, and we take that very seriously. It is a major part of the way that we construct our technology. And so any breach of that type is of paramount concern to us.

Mr. JOHNSON. Well, if the same technology used by the Department of Defense to protect its own internal security, cybersecurity issues, if that technology were used to do the reverse to a private citizen of America, that would not be a proper use of DOD techniques, would it?

Ms. TAKAI. Well, again, any breach, and any malicious software or hardware, or any breach to DOD information——

Mr. JOHNSON. Well, no, I am not talking about DOD information; I am talking about DOD information being used against American citizens for the use of private entities.

Ms. TAKAI. Again, I am not familiar with any particular instances of that. Certainly if there are areas that we can research and take a look at, then we would be very happy to do that and get back to you.

Mr. JOHNSON. Well, again, I would like to request copies of any and all contracts between the Department of Defense and the three subcontractors or the three contractors that I mentioned, HBGary Federal, Palantir Technologies, and Berico Technologies. Would you be able to provide me with that information, and also the chairman of the committee?

Ms. TAKAI. I don't have that information directly myself, but certainly again I will have staff research that, and we will get back to you with an answer to that question.

Mr. JOHNSON. Well, I think it is a very important issue that I am not planning on sweeping under the rug. I want to at least get those contracts and analyze them to determine whether or not they have been used or they have been breached. So I need that information.

Ms. TAKAI. Yes, sir. Again, we will have my staff research it, and we will get back to you with an answer.

Mr. JOHNSON. Thank you.

Anything you can add, Ms. McGrath?

Ms. MCGRATH. No. I do not have my own self familiarity with the proposal nor those three companies. Certainly the contracts are written in accordance with the Federal Acquisition Regulations, and we would have to look at the scope and conditions of each one of those to make sure that there is not a breach of contract. But I do not see an issue with complying with your request to have cop-

ies of those contracts, and I will ensure that Ms. Takai has all the support she needs to get those.

Mr. JOHNSON. Well, Ms. Takai, I tell you, while I was asking you some questions, out of the corner of my eye, I saw somebody come up and give you a note, and that always kind of arouses my curiosity. I won't ask you what is in it, but I am concerned about this case and the way it is being swept under the rug.

Thank you, Mr. Chairman.

Mr. THORNBERRY. Mr. Conaway.

Mr. CONAWAY. Recognized for 7, 8 minutes? Excuse me.

Ms. McGrath, thank you.

Ms. Takai, thank you for being here.

You talked to us about the impact that the—I am blanking on the name—the $100 million reprogramming exercise that DOD went through to try to find $100 million in monies that they would put other places within the system itself, what impact that had on the efforts to get the Department of Defense's financial statements audited. Did it hurt, helped?

Ms. MCGRATH. To be clear, the $100 billion efficiency initiative. I think we all wish it was $100 million and not $100 billion.

The Department, as certainly the members of this committee are well aware, took an initiative with Secretary Gates leading to look for efficiencies in all aspects of not only the way we do business, but what we are procuring, how we are procuring it, how we are organized; you know, are we positioned to be the most efficient and effective organization that we can be, and to look for opportunities to identify efficiencies.

Mr. CONAWAY. But how did it—help or hurt?

Ms. MCGRATH. So I think that some of the lasting impacts of the efficiency initiative we won't know until we are actually realizing some of those efficiencies. We have identified the opportunities for those efficiencies. I can talk——

Mr. CONAWAY. Well, let me ask the question this way. Do you have the accounting systems, internal control systems, and management systems in place to actually track that $100 billion and know that it went from one spot to the other?

Ms. MCGRATH. So we have the mechanism in place, will be led by Secretary Lynn, with Mr. Hale, our comptroller, and myself looking at—and with the Under Secretaries of the military departments leading the data collection, if you will, for their organizations, along with their CFOs [Chief Financial Officers], to ensure that we understand the—I will say how close we got to the efficiencies that we identified.

So from a systems perspective, I want to be clear, I think we have the governing structure in place to ensure that we can accurately identify the efficiencies.

Mr. CONAWAY. Then why can't we audit that governance structure?

Ms. MCGRATH. Some of the data collection that we will utilize will not be 100 percent systems-based. It will require a combination of both manual and IT, if you will, to enable the data collection. And I think that you are aware that from an auditability perspective, if you put people on a problem or an initiative like

auditability, you don't have a sustained process. And the path the Department is pursuing for auditability is one of sustainment.

Mr. CONAWAY. I can't put words in your mouth. I am doing a pretty poor job of it. If you had better systems in place, would there be less manhours required to manually track the $100 billion? Because if you are using manhours to put together one-time schedules that track that big nut, that is the least efficient way to do it. You get it done, and perhaps the numbers would be good. But if you had better systems that spoke as you talk, end to end and across the systems and all those buzzwords that MBA [Masters of Business Administration] guys who write these papers use currently, that current lexicon, would it be easier to do that? Would it be easier to do the $78 billion in cuts in terms of trying to find those?

Ms. MCGRATH. Yes.

Mr. CONAWAY. Thank you. I appreciate that.

Because much of this auditability does rely around the purchase of systems, and we have had these age-old issues of one branch likes one general ledger package, and another branch likes a different one, can you talk to us about progress that you are making in helping, you know, one common HR [human resource] system, one common fixed-asset handling system, those kinds of things, in order to gain efficiencies, and to do it the way an enterprise would do it versus stand-alone subsidiaries, as an example of the business?

Ms. MCGRATH. So the Defense Department, being as large and complex as it is, we have multiple systems that establish transactions to then feed into the broader general ledger system. We are pursuing, I will say, five main financial systems, one for each of the services and then the defense agency-wide initiative. We are also taking a standards-based approach to ensure that we have commonality of data, the standard financial information structure, so that we can aggregate the information at the end of the day.

It is not just those financial systems, as you mentioned. It is the logistics systems, it is the personnel systems, and again ensuring that they have the financial standards in them so that when we feed from a transactional level up to the financial, then we can aggregate the information.

Mr. CONAWAY. If the chair will indulge me. You have got to have some system to track progress against that. We need to have oversight on the success of what you are doing. We are not going to do what you have to do, we are just simply asking you to do it. And so perhaps off-line conversations about how you satisfy yourself as the person responsible, or one of the folks responsible, for making this happen, that you are on task, on time to make that 2017 deadline, which I think we all want to, which is systems in place that are sustainable and, oh, by the way, auditable and audited.

Thank you, Mr. Chairman. I yield back.

Mr. THORNBERRY. Thank you.

Ms. Takai, in answering some of Mr. Langevin's questions a few minutes ago about some of the tools you are putting in place to prevent WikiLeaks-like things, one of the things you mentioned was a new tool to detect anomalies. Surely there is commercial products very suited to that. I mean, every time you go overseas and use your Visa card, they call, for example.

Ms. TAKAI. Yes, sir. The tool that we are looking at is a commercial product. And what we are doing is testing the integration of that product with our Host-Based Security System to ensure that, again, we have that integration.

The second thing with any commercial tool is that we have to do a level of testing, because the volume and the size of our implementations are generally larger than what any of the tools are doing in the commercial space. So we always take a look and make sure that we have scalability in those tools. But in this particular case, that tool is a commercial-off-the-shelf product, yes.

Mr. THORNBERRY. You mentioned a few minutes ago as $38 billion, roughly, in the accounts we are looking at; $2.8 billion, I think you said, for information assurance kinds of things. Is that enough?

Ms. TAKAI. Well, we are looking at that. In fact, it is interesting that you would ask that question, because Secretary Gates actually also asked us that same question as we were relating to him the review of what we are doing from an insider threat mitigation standpoint.

Certainly for the calendar year, we believe that that $2.8 billion will successfully allow us to implement the tools that I mentioned, as well as helping us to look at some of the emerging threats and what we need to do.

I think one of the things that is important to know is that improving our security isn't totally in just what we spend under the cybersecurity label. The things that we are doing around standardization of our infrastructure actually are all, if you will, cybersecurity investments, but are not labeled as such. So to some extent, when we talk about that spending, it isn't totally representative of everything we are doing.

Mr. THORNBERRY. Fair point. Fair point.

I think we have run out of questions for the moment. Thank you both for being here and for answering questions on a wide variety of topics. We look forward to continuing to work with you both towards the things you are trying to achieve.

With that, the hearing is adjourned.

[Whereupon, at 4:12 p.m., the subcommittee was adjourned.]

A P P E N D I X

APRIL 6, 2011

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

APRIL 6, 2011

Opening Remarks of
Ranking Member James R. Langevin
For the Emerging Threats and Capabilities Subcommittee
Hearing on
Management of DoD IT Acquisition Systems

April 6, 2011

Thank you, Mr. Chairman. I would also like to welcome our witnesses today. It is good to have the Honorable Elizabeth McGrath and the Honorable Teresa Takai here and I look forward to their testimony.

The issue of Information Technology is critically important to the Department of Defense and I want to thank Chairman Thornberry for calling this hearing. IT is a crucial factor in every aspect of the Department's activities. From routine email to the flight controls of the most sophisticated jet fighters in the world, the Department depends on the smooth functioning of myriad IT systems. As the information age matures, we find that IT systems have expanded in both complexity and pervasiveness. As a result, today they represent one of the largest investments for the Department – and they present a significant potential vulnerability if they should fail or be attacked. The business complexities are only made worse by the evolving cyber threats that have begun to challenge the integrity of our current systems.

Therefore, it is important for the Department to be properly organized to pursue IT acquisition, implementation, modernization and performance evaluation. Oversight is required for the full spectrum of activities, but bureaucratic redundancy creates confusion and complexity. The DoD IT enterprise must be as streamlined and efficient as possible. I understand that as part of the Secretary of Defense's efficiency initiative, we will see some changes in how the Department manages IT, and perhaps some cost savings. This is welcome news, provided it achieves the desired effect without reducing capability or injecting unnecessary risk into the process. But we must also be vigilant that as we move forward, the security of our systems is at the forefront of our efforts.

Our acquisition systems, furthermore, are barely suitable for large scale weapons projects – requirements for IT systems evolve much more rapidly, and the system needs more flexibility if it is to manage the proper acquisition of these systems. [As Mr. Thornberry mentioned,] Last year's 2010 National Defense Authorization directed the DoD to develop and implement a new acquisition process for IT and I look forward to hearing about how that is proceeding today.

HOLD UNTIL RELEASED BY THE
HOUSE ARMED SERVICES SUBCOMMITTEE ON
EMERGING THREATS AND CAPABILITIES

STATEMENT BY

THE HONORABLE ELIZABETH A. MCGRATH

DEPUTY CHIEF MANAGEMENT OFFICER

BEFORE THE

House Armed Services Subcommittee on
Emerging Threats and Capabilities
April 6, 2011

HONORABLE ELIZABETH A. MCGRATH
DEPUTY CHIEF MANAGEMENT OFFICER
SUBMITTED STATEMENT
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES
WEDNESDAY, APRIL 6, 2011

Mr. Chairman, Congressman Langevin, members of the Subcommittee:

Thank you for the opportunity to discuss the Department of Defense's efforts to improve its business operations and, specifically, its acquisition and management of business Information Technology (IT) systems. As the Department of Defense Deputy Chief Management Officer, I am the Deputy Secretary of Defense's primary agent for integrating and improving our critical business operations. I am responsible for instituting a framework to define clear business goals, create meaningful performance measures and align activities via established and repeatable processes. The purpose of DoD's overarching management agenda, and the focus of the work undertaken by my office, is establishment of an effective, agile and innovative business environment that is fiscally responsible. There are a number of on-going efforts that are crucial to achieving this agenda, and today, I would like to highlight not only our IT acquisition reform efforts and other business IT initiatives, but also some successful, cross-agency management efforts that are well underway.

End-to-End Defense Business Operations

We have embarked upon, for the first time ever, a significant initiative to optimize the "end-to-end" business processes used throughout the Department. Fundamentally, the Department's business IT systems are essential **enablers of a broader set of integrated business operations,** rather than ends unto themselves. Too often, there is an inclination to jump straight to a material solution to solve a business problem without first thinking about the

problem holistically. Taking a more comprehensive view of the business environment requires us to think differently. **We must approach our business as a cross-functional, integrated enterprise** comprised of a series of end-to-end processes, rather than individual stove-piped organizations performing specific and oftentimes disconnected business functions. For example, paying our Service members on-time is a shared responsibility among numerous members of our enterprise; including human resources and financial professionals. Additionally, it is not an issue that can be addressed solely through new IT systems; but instead requires reform of our processes, governance, and policies. Similarly, achieving financial auditability within DoD is a shared responsibility across multiple business domains (e.g., contracting, real property and supply chain), not just the financial management community.

To establish a framework for thinking about our business in this way, we identified 15 essential end-to-end processes, such as Hire-to-Retire and Procure-to-Pay. These end-to-end processes are represented in our Strategic Management Plan and Business Enterprise Architecture, and our senior governance bodies have embraced and are managing within the end-to-end construct to identify the sub-processes, systems, data standards, performance measures and laws, regulations, and policies necessary to improve our business and drive better IT implementations. This more holistic understanding of our business will allow us to make more informed Enterprise-wide decisions. It will also allow us to make targeted investments in business IT capabilities and ensure those investments are interoperable, efficient and non-duplicative - regardless of whether those investments are Enterprise or component systems, Enterprise Resource Planning (ERP) systems or distributed services.

We have already made progress in this area, by focusing on process improvement first, and then ensuring the right tools and governance structures are in place. Our Business Enterprise

Architecture is maturing and serves as a tool that guides our investment decisions as well as aligning the Department to common standards and approaches. Our investment management process, from our Invest Review Boards to the Defense Business System Management Committee (DBSMC) provide us the ability to ensure planned investments fit the target environment, align to the architecture and have successfully undertaken business process reengineering. These efforts, coupled with our on-going work to reform acquisition of information capabilities is delivering better results for the business operations our Warfighters depend upon.

A key critical enabler to the integrated approach of our significant transformation opportunities is integrated and effective governance. The DBSMC is the corporate governance board for our business operations and establishes goals, processes, policies and management practices that enable efficient and effective business outcomes. The DBSMC endorses the integrated end-to-end approach that will serve as a catalyst for change. Additionally, there are subordinate governance bodies focused on specific business areas that understand the importance of thinking through our business using an end-to-end lens. For example, the Financial Improvement and Audit Readiness Governance Board, that I co-chair with the Department's Comptroller, oversees progress toward achieving financial auditability and will use end-to-end processes to understand the non-financial aspects of our business that must change in order to reach our stated audit goals. The Investment Review Boards will use the end-to-end construct to guide business related IT investments versus making investments in stove-piped capabilities that sub-optimize the overall business objectives of the Enterprise.

Though these planning activities are critical to sustained long term success, they are not enough. I have charged the business mission area of the Department to use the end-to-end

framework as a reference for rationalizing our current business IT investments. We are starting with the end-to-end process for Procure-to-Pay and using a multi-phased approach to evaluate our existing portfolio to determine which investments fit best with our business strategy and which investments to brown out or sunset.

IT Acquisition Reform

While an integrated end-to-end focus and strong governance are critical to success, a new approach to organizing our business is not enough. We must change our approach to acquiring information capabilities. There has been no shortage of studies and reports, including one by this Committee last year, that concluded the Department's method for acquiring IT systems takes too long, costs too much, and does not always deliver the desired capability to users. Steps are being taken to address these problems.

Section 804 of the Fiscal Year (FY) 2010 National Defense Authorization Act directed DoD to develop and implement a new acquisition process for IT systems that included greater user involvement, incremental capability releases and improved governance. In response to this requirement, the Department established an IT Acquisition Task Force. The Task Force, which I chair, includes extensive participation from across the Department and is regularly engaged with key stakeholders within DoD and industry, to identify and deliver significant reforms. The IT Task Force is charged with addressing the unique challenges associated with the different types of IT the Department relies on – warfighting systems, infrastructure, communications and command and control systems and defense business systems.

The guiding principles adopted by the IT Task Force incorporate several recommendations from the Defense Science Board Report and include:

- Deliver Early and Often, with Delivery of Capability in 12 to 18 months
- Incremental and Iterative Development and Testing
- Rationalized Requirements
- Tailored and Flexible Processes
- Knowledgeable and Experienced IT Workforce

These principles, as well as the approach the Department is taking, are outlined in more detail in the November 2010 Report, "A New Approach for Delivering Information Technology Capabilities in the Department of Defense," submitted to Congress last year. As stated in the report, we have formed a number of working groups to address specific elements of the acquisition process, including governance, requirements, portfolio management, contracting, funding, acquisition process, testing, workforce, architecture and metrics. Areas we are addressing include but are not limited to: establishing a robust set of metrics that include leading indicators to assess overall health of a program; combining certification and accreditation with traditional test and evaluation activities; and assessing contracting strategies that enable more modular delivery of capability. Recommendations from our work groups are being reviewed by members of the IT Task Force and consolidated into a draft policy that we expect will be promulgated this summer. The Department is using a pilot-based approach to validate the new policy and will modify it as necessary based on lessons learned prior to final issuance.

Defense Business System IT -- Acquisition Reform Efforts Underway

While I support our longer term strategic acquisition reform initiatives, I think it's important to test these changes to business system acquisitions to ensure our proposed policies and approaches are working. On November 15, 2010, the Under Secretary of Defense for Acquisition,

Technology and Logistics (USD(AT&L)) signed a new acquisition policy for defense business systems, the Business Capability Lifecycle or BCL. BCL provides a streamlined framework for structuring definition, development, testing, production, deployment and support of defense business IT systems. It consolidates oversight requirements (i.e., funding, requirements and acquisition) into one integrated structure, the Investment Review Board, while streamlining documentation requirements. The principle focus of BCL is program implementation.

Using BCL and the tenets of IT reform as a reference point we challenged the Air Force to propose an acquisition approach that would deliver capabilities for the Defense Enterprise Accounting and Management System (DEAMS) in 18 month increments. DEAMS is a financial management initiative that will transform business and financial management processes and systems to provide accurate, reliable and timely business information in support of effective business decision making for the Air Force and U.S. Transportation Command. DEAMS recently completed a technology demonstration and is positioned to be deployed throughout the Air Force. Originally, DEAMS was structured as a traditional weapons system acquisition and as such the program office proposed a schedule that would deliver DEAMS capability to the Air Force no later than 2017, with an initial DEAMS release in 2014. This schedule did not meet Air Force goals to achieve auditable financial statements.

The program office, in close coordination with its functional sponsor and the Air Force Deputy Chief Management Officer, initiated a requirements validation effort and reordered program priorities to leverage completed development activities. Using these reordered priorities, the program office proposed a streamlined acquisition approach with the potential to field initial DEAMS capability as soon as 2012 and full DEAMS capability by 2015, two years earlier than previously projected. DEAMS presented their approach to me as the Milestone

Decision Authority via the Investment Review Board process and I approved their strategy and asked the program office to propose an acquisition strategy consistent with the proposed accelerated approach.

Cross-Agency Reform Efforts

The following two examples highlight business IT efforts that embrace our end-to-end approach and the tenets of IT acquisition reform: our efforts in Electronic Health Records (EHR) and security clearance reform.

To successfully address today's challenges, **we must approach our business as a cross-functional, integrated enterprise.** We have discovered that sometimes we must also approach business as a cross-agency undertaking. While this requires engaged senior-level participation from across the government, the results are greatly encouraging. The following two examples of work being led by my office illustrate what will and can be done when we reform business operations across agencies.

In the field of health IT, DoD and the Department of Veterans Affairs (VA) have committed to a full and seamless electronic exchange and record portability of healthcare information in a secure and private format, wherever needed, to ensure the highest quality and effective delivery of healthcare services for our Military Service members and Veterans, from their accession into Service and throughout the rest of their lives. To this end, the Departments are collaborating on a common framework and approach to modernize our Electronic Health Record (EHR) applications. On March 17th, the Secretary of Defense and Secretary of Veterans Affairs affirmed we will continue to synchronize our EHR planning activities to accommodate

the rapid evolution of healthcare practices and data sharing needs, and to speed fielding of new capabilities. The Departments have already identified many synergies and common business processes, including common data standards and data center consolidation, common clinical applications and a common user interface.

In the area of personnel security clearances the Department, led by my office, invested significant effort on improvement of personnel security clearance processes, both within the Department and as part of an integrated federal reform effort. In 2005, the Government Accountability Office (GAO) placed the Department of Defense Personnel Security Clearance Program on its High Risk List due to serious timeliness issues, which included extensive backlogs and significant delays in the clearance process. Each year since then, we have taken proactive steps and made incremental improvements. This included direct leadership engagement, sufficient resources to resolve risk, a corrective action plan, presence of a program to monitor and independently validate effectiveness and sustainability of corrective actions and the ability to demonstrate implementation of corrective measures.

The work required a concerted, long term effort by DoD, the Office of the Director of National Intelligence, the Office of Personnel Management and the Office of Management and Budget, the results of which have been truly noteworthy. As a point of reference, the executive branch in Fiscal Year 2006 averaged 165 days to complete a security clearance investigation. The bulk of those actions can be attributed to DoD, which accounts for approximately 87 percent of that workload. As of the fourth quarter of FY 2010, 90 percent of investigations and adjudications for DoD were completed in an average of only 47 days. This performance is attributable to a thorough assessment of the end-to-end process and the development and deployment of our automated Case Adjudication and Tracking System (CATS). CATS

eliminated unnecessary caseworker intervention in over 70,000 cases last year alone, and was a key factor in reducing clearance adjudication time from over 70 days in FY 2009 to an average of 9 days in the fourth quarter of FY 2010. Begun as an Army IT pilot, CATS is now Web-based and used DoD-wide. It will soon be adopted as a Web service by other agencies, including the Department of Energy. The progress made in security clearance processing was so significant that, in February this year, the issue was removed from the GAO High Risk List.

Closing

In closing, the Department is committed to improving management and acquisition of IT systems and as well as its overall business operations. These issues receive significant management attention and are a key part of our overarching strategy to build better business processes that will create lasting results our men and women in uniform need, and that you and our taxpayers expect. I look forward to continuing our work with this Committee in the months and years ahead as we work toward greater efficiency, increased effectiveness and further agility in the business space of the Department, enabled by modern, interoperable IT capabilities.

I look forward to your questions.

Elizabeth A. McGrath

Deputy Chief Management Officer for Department of Defense

Ms. Elizabeth (Beth) A. McGrath was sworn in as the Department's first Deputy Chief Management Officer, a Senate-confirmed and politically appointed position, on July 1, 2010. Ms. McGrath leads the Department's efforts to better synchronize, integrate and coordinate DoD business operations and serves as the Principal Staff Assistant (PSA) and advisor to the Secretary and Deputy Secretary of Defense for matters relating to management and improvement of business operations. Ms. McGrath is focused on achieving sustainable and enduring improvements and efficiency and effectiveness in the Department's business related enterprise policies, processes and systems. She also serves as the DoD Performance Improvement Officer and is responsible for formulating the legislatively mandated Departmental Strategic Management Plan.

Ms. McGrath serves as the Milestone Decision Authority for numerous business-focused Major Automated Information Systems (MAIS) and also executes the Department's primary governance body for business transformation, the Defense Business System Management Committee; establishes performance goals and measurements for the Department's business operations; implements the Department's Continuous Process Improvement efforts; and is the Vice-Chair of the Performance Accountability Council that is responsible to the President to reform the government-wide security clearance process. Her responsibilities require extensive integration and coordination across the Department as well as with many Federal agencies, such as the Office of Management and Budget, Director for National Intelligence and the Department of Veterans Affairs.

Previously, Ms. McGrath served as the Deputy Director for Systems Integration, Defense Finance and Accounting Service (DFAS) where she created a financial migration strategy that was executed with a collective budget of approximately $1B. She managed the entire financial architecture supporting DoD-wide standard financial systems, integrating it with the Department's evolving target, enterprise architecture. Project scope included logistics, personnel, medical, acquisition and financial missions including many information technology solutions.

Prior to joining DFAS, Ms. McGrath served in a variety of program management roles culminating in Program Executive Office-level oversight responsibility. She possesses extensive knowledge of acquisition-related statutes, regulations and policies with over 20 years applied acquisition experience with Major Defense Acquisition Programs and MAIS. She served as the Business and Acquisition Manager on an international torpedo defense program with the United Kingdom and held numerous other financial, acquisition and program management positions within the Department of the Navy.

Ms. McGrath was awarded the Meritorious Executive Presidential Rank Award for Fiscal Year 2008 and the Office of the Secretary of Defense Exceptional Civilian Service Award in October 2008. She

holds a bachelor's degree in Economics from George Mason University, is a graduate of the Federal Executive Institute, is certified Acquisition Level III in Program Management, Financial Management and Logistics and is a member of the DoD Acquisition Professional Community.

STATEMENT BY

TERESA M. TAKAI
ACTING ASSISTANT SECRETARY OF DEFENSE
FOR NETWORKS AND INFORMATION INTEGRATION
AND
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON
EMERGING THREATS AND CAPABILITIES

ON

IMPROVING MANAGEMENT AND ACQUISITION OF INFORMATION TECHNOLOGY SYSTEMS IN THE DEPARTMENT OF DEFENSE

APRIL 6, 2011

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
SUBCOMMITTEE ON EMERGING THREATS
AND CAPABILITIES,
HOUSE ARMED SERVICES COMMITTEE

Good afternoon Mr. Chairman and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee on Emerging Threats and Capabilities on the importance of information technology (IT) to the transformation of the Department of Defense (DoD). I am Teri Takai, and I am the Acting Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) and the Department's Chief Information Officer (CIO). My testimony today will focus on how the DoD is leveraging information technology to securely deliver mission critical information capabilities to the men and women of the Department of Defense and our mission partners.

Department of Defense Information Technology (IT) Overview

The Department's FY12 IT budget request of $38.4 billion includes funding for desktop computers, tactical radios, identity management technology, commercial satellite communications, and more. These investments support mission critical operations that must be delivered in an environment of ever-changing requirements and ever-increasing demand for additional information capability. Where in the past the Department sought to balance the "need to know" with the "need to share," today, the warfighter expects to have and needs to have the latest information in order to complete the mission. The increasing use of social media, smart phones and tablet computers has made information sharing an expectation. This expectation requires new capabilities, particularly in the "edge" or tactical environments that have limited availability to persistent, high speed

connections. Our challenge today is ensuring our networks can securely support the information demands of our users – users who require access to information anywhere and anytime across the DoD Information Enterprise (IE), allowing them to make informed decisions in the execution of their missions. To meet this challenge, DoD networks must be designed and optimized to more effectively and efficiently support mission operations, for both garrisoned users and those at the "edge".

Information Assurance or Cybersecurity. DoD networks are under constant attack from cyber security threats launched from the Internet or from malicious software embedded in email attachments, removable media, or embedded in the hardware the Department procures. Every device connected to the network is susceptible to cyber vulnerabilities. While working to efficiently respond to the information demands of our users, we must be ever vigilant in protecting our information environment from cyber threats.

Just over $2.8 billion of the Department's $38.4 billion IT budget request is devoted to information assurance or cybersecurity activities that defend the Departments information, information systems and communications networks. The Department's FY 2012 information assurance budget request includes increased funding to address insider threat and cyber vulnerabilities such as those identified in the WikiLeaks incident, among other things. Specifically, we have requested funding to support deployment of a Public Key Infrastructure (PKI)-based identity credential on a hardened smart card for use on the Department's secret classified network, a successful technology very similar to

the Common Access Card (CAC) we use on our unclassified network. We have also identified funds needed to: deploy Host Based Security System (HBSS) to secure our classified systems; provide an automated capability to continually monitor the configuration and security state of DoD networks; and improve identity management capabilities across the Department.

Operational Efficiencies. The DoD is planning for the investment and implementation of these IT and information assurance capabilities within today's current resource constrained environment. Recognizing this budget environment, in August 2010, the Secretary directed a number of initiatives to achieve savings in acquisition, sustainment, and manpower costs, while not degrading the Department's ability to execute its missions. Among these is the consolidation of the Department's IT infrastructure while simultaneously defending that infrastructure against growing cyber threats.

DoD IT Enterprise Infrastructure Optimization Strategy and Plan

My office is responsible for leading the development of a strategy and plan for consolidating the Department's IT infrastructure in five (5) broad areas: network services; computing services, application and data services, end-user services, and IT business processes. I plan to issue the DoD IT Enterprise Infrastructure Optimization Strategy and Plan this quarter. This plan represents the Department's strategy and initial roadmap to achieve the goals of improving mission effectiveness and heightening the Department's security posture. By delivering a streamlined, rationalized, and simpler

network through consolidation of information technology infrastructure across the Department, this strategy will deliver efficiencies that can be redirected to mission capabilities. This plan commits us to changing policies, cultural norms, and organizational processes to provide lasting results. The initial focus is on obtaining tangible results in Fiscal Years (FY) 2011-2012, while planning for aggressive consolidation through FY 2015. This consolidation will make us better positioned to embrace emerging technology and provide cutting-edge capabilities to our warfighters. It is intended to provide the Department with the flexibility required to respond to and incorporate emerging technologies, while taking corrective action on those efforts not producing required results.

The result of these consolidation initiatives will be a DoD Information Environment that provides the warfighter with the required information and services needed to accomplish their mission. This standardized information and network infrastructure will eliminate the organizational barriers to information sharing and eliminate seams which attackers can exploit to gain access to vital information or systems. It will also increase the flexibility of defense networks to incorporate or respond to changes in emerging technology by minimizing the disparity within the Department's information architecture.

IT Investment Planning

The transformation of DoD's IT capabilities described above is a very ambitious undertaking – one that will reap tremendous benefits to the Department and our Nation

when completed. It will require agility, as well as new processes, to both keep abreast of technological advances and defend the network against emerging cybersecurity threats.

In particular, changes to the Department's three core processes (requirements, budgeting, and acquisition) are required to address the systemic conditions resulting in DoD's stove-piped IT infrastructure. My office is working closely with the office of the Deputy Chief Management Officer on efforts to develop a flexible, agile acquisition process that also addresses the DoD's requirements and budgeting processes to institutionalize the agility and flexibility necessary in this rapidly evolving domain.

IT Workforce

The Department recognizes that the development, education and continuous training of our workforce is critical to ensuring the success of our IT and IA investments, and essential to our ability to utilize new capabilities and defend against emerging threats. I work closely with the office of the Under Secretary of Defense for Personnel and Readiness on that objective and I am working closely with other elements of the Department to ensure that we understand the evolving IT and IA workforce needs of the Department.

The Information Technology Exchange Program (ITEP) pilot, reauthorized by the FY 2010 National Defense Authorization Act for DoD, is one mechanism that the Department is pursuing to that end. Under this collaborative learning venture, DoD and

private industry organizations share best practices through the exchange of high performing personnel in IT functional areas such as IT Acquisition and Information Assurance (IA). ITEP provides an opportunity for both industry and the Department to learn from each other – to enhance employees' IT competencies and technical skills and infuse both DoD and industry with new ideas in this fast-evolving discipline. The program allows private company IT and IA employees to be detailed as employees to the DoD, with the private company continuing to pay the employee's salary. Similarly, DoD IT and IA professionals could be detailed to the private sector to gain experience; these employees would remain federal workers and their salaries would be paid by the DoD.

Through this exchange program, industry and government can gain a better understanding each other's IT management policies and procedures. The program will strengthen IT competencies and skills of employees from both federal and private sectors, and has the opportunity to change the dynamics of the way the public and private sectors share best practices and knowledge in the future.

My Office is responsible for implementing ITEP and we have created a guide to assist participating DoD Components with the implementation. The Department's goal is to have ITEP pilot participants on board by June 2011. In October 2011, we will formally report to the Congressional defense committees on the implementation and benefits of the program in the first of a series of annual reports.

Summary

Maintaining an information advantage for our users is critical to our national interest. The efforts outlined in this brief will ensure that the Department's information capabilities provide better mission effectiveness and security, and are delivered in a manner that makes the most efficient use of financial resources. My job is to provide the vision and leadership within the Department to ensure that these efforts satisfy the users' requirements effectively, efficiently and securely.

I want to thank you for your interest in our efforts and I am happy to answer any questions you may have.

TERESA M. TAKAI

Acting Assistant Secretary of Defense for Networks and Information Integration / DoD Chief Information Officer

Teri Takai is the Acting Assistant Secretary of Defense for Networks and Information Integration and the Department of Defense Chief Information Officer (ASD (NII) / DoD CIO). She serves as the principal advisor to the Secretary of Defense for Information Management/Information Technology and Information Assurance as well as non-intelligence Space systems, critical satellite communications, navigation, and timing programs, spectrum and telecommunications. She provides strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology based capabilities required to support the broad set of Department missions.

Ms. Takai previously served as Chief Information Officer for the State of California. As a member of the Governor's cabinet, she advised the governor on the strategic management and direction of information technology resources as the state worked to modernize and transform the way California does business with its citizens.

As California's CIO, Ms. Takai led more than 130 CIOs and 10,000 IT employees spread across the state's different agencies, departments, boards, commissions and offices. During her tenure as State CIO, Teri pursued an agenda that supports viewing California's IT operations from an enterprise perspective, including: Forming a Project Management and Policy Office, release of the California Information Technology Strategic Plan, passage of the Governor's IT Reorganization Proposal, establishing a Capital Planning Process and directing agency consolidation activities.

Prior to her appointment in California, Ms. Takai served as Director of the Michigan Department of Information Technology (MDIT) since 2003, where she also served as the state's Chief Information Officer. In this position, she restructured and consolidated Michigan's resources by merging the state's information technology into one centralized department to service 19 agencies. Additionally, during her tenure at the MDIT, Ms. Takai led the state to being ranked number one four years in a row in digital government by the Center for Digital Government. Additionally, in 2005, Ms. Takai was named "Public Official of the Year" by *Governing* magazine. She is also Past-President of the National Association of State Chief Information Officers and currently serves on the Harvard Policy Group on Network-Enabled Services and Government.

Before serving in state government, Ms. Takai worked for the Ford Motor Company for 30 years, where she led the development of the company's information technology strategic plan. She also held positions in technology at EDS and Federal-Mogul Corporation. Ms. Takai earned a Master of Arts degree in management and a Bachelor of Arts degree in mathematics from the University of Michigan.

○